6 May 1983

MEMORANDUM FOR: Director, Intelligence Community Staff

FROM: Deputy Director of Central Intelligence

SUBJECT: Minimum Computer Security Standards

1. I would like you to develop "Community-coordinated minimum acceptable computer security standards." These would then be applied to any Community computer networks that we might develop. You might want to consider the DoD Computer Security Evaluation Center's criteria for computer security as a starting point.

2. Please advise how much time you think you will need to complete this effort.

25X1

25X1

John N. McMahon

25X1

SECRET

DCI/ICS 83-4383
6 June 1983

MEMORANDUM FOR: Deputy Director of Central Intelligence

25X1

FROM: [redacted]
Director, Intelligence Community Staff

SUBJECT: Minimum Computer Security Standards

REFERENCE: Your Memorandum dated 6 May 1983; Same Subject

1. Minimum standards regarding computer security are probably the most difficult to determine. We need to balance a good understanding of the vulnerabilities and the threat coupled with some agreed upon tolerable level of "risk." We do not have the knowledge or experience to do so at the present
25X1 time. [redacted]

2. Formal computer standards generally require five to seven years to develop, to coordinate, and to introduce effectively into the infra-structure. In general, technical criteria are relatively easy to prepare and even to reach agreement upon. Policy implications (turf), compliance
25X1 auditing, and cost (whose budget) are issues that take longer. [redacted]

3. I suggest a dual approach which will provide rapid improvements and will permit early applications, along with a longer term effort. The imposition of standards is expensive and, if they are mandatory, will be even more costly. This dual approach equates to setting near-term action priorities with specific follow-through on supporting the associated costs, and in a more deliberate pace, to develop and coordinate the more broadly
25X1 applicable standard or standards through the existing mechanism of the Computer Security Subcommittee of SECOM under the applicable DCIDs. [redacted]

4. An approach which appears practical and likely to reduce vulnerabilities of "critical" systems on a "fast-track" basis would be described as follows:

a. Identify those few critical systems which must meet a set of mandatory standards; for systems not designated as critical, impose the standards as voluntary for a transition period. This will allow budgets to "catch up" with the costs of imposed standards.

b. Specify a set of vulnerabilities which by any criteria generate the greatest threat and highest risk; develop, promulgate and impose mandatory standards that will reduce these high threat and risk areas to an acceptable threshold.

25X1

WARNING NOTICE
INTELLIGENCE SOURCES
OR METHODS INVOLVED

SECRET

[redacted]

c. Set up Task Groups to generate proposed policies and standards--mandatory in some cases, voluntary in others; as soon as the scope of each standard is sufficiently defined, determine schedule and costs of implementation and means for validating adherence.

25X1

5. The vulnerabilities which generate the greatest risk are at the same time amenable to "quick-fix" improvements. The proposed areas to be considered are:

a. Access Procedures

- By individuals through terminals across networks to remotely located data bases.
- By individuals who directly access "computer centers" and data bases (either on-line or off-line).
- By regular computer-to-computer transfer of information without scheduled manual checks.

b. Dissemination or Security Control "Labelling" of Information

- Upon entry to computer data bases.
- When transmitted from or produced by computer systems for any purpose over any media.

c. Dissemination or Security Control Accountability

- Presently, there appears to be no automatic accountability system to monitor and serve as record keeper for computer-based information storage and retrieval systems. Such systems are an absolute necessity if any measure of electronic information security is to exist.

25X1

- Guidelines for such automatic accountability and requirements for developing automated accountability are the practical first surrogates for standards in this instance.

25X1

6. Existing organizational or committee structures can and should be used to develop these first highest priority set of Critical Electronic Information Security Standards and Guidelines. IHC, SECOM, CI, ISS, CSEC and the DIA DODIIS Office are among the best candidates for handling these tasks, and there is a natural split of responsibility among the proposed Critical Set of Standards and Guidelines.

25X1

7. If the basic approach outlined above is acceptable to you, then some first products could be off the drawing board in about 90 days. I would like to discuss this further with you and to include [redacted] 25X1
[redacted] We will then proceed to get agreement from our newly formed ELINFOSEC 25X1
Steering Group (ESG). (U)

[redacted] 25X1

Rear Admiral, USN

SECRET

25X1

The Director of Central Intelligence

Washington, D.C. 20505

NFIC-9.11/1
22 January 1985

MEMORANDUM FOR: See Distribution

SUBJECT: Reports on Computer Security for SCI-Handling Systems

1. The DCI's Computer Security (COMPUSEC) Project began in April 1983 and is intended to support the DCI in assessing the security of automated systems processing information derived from sensitive methods and sources, to identify the threats to automated systems processing such materials, and to recommend actions for the DCI that will allow him to attest to the acceptability of operating risks.

25X1

2. As part of the DCI's COMPUSEC Project, the COMPUSEC Project Team developed an assessment on the threat to US automated Intelligence Community systems (See Attachment 1). Representatives from the NFIC Community have provided input to this document. This formulation of the "threat" is being used in conjunction with security assessments of the Intelligence Community's "critical" automated SCI systems to set program and budget priorities for immediate security upgrades. This threat point paper also serves to fulfill one of the DCI's continuing distinctive responsibilities.

25X1

3. The SAFEGUARDS document (Attachment 2) identifies security requirements for the protection of SCI information in the "critical" systems evaluated as part of the DCI's Computer Security (COMPUSEC) Project. When fully implemented in the "critical" systems, the SAFEGUARDS will correct the security shortfalls and reduce to an acceptable level the risks currently associated with processing this sensitive information in the "critical" systems. I intend to direct that the SAFEGUARDS be imposed as mandatory standards for the 13 "critical" SCI-handling systems by the end of FY 86. These SAFEGUARDS will also be imposed as voluntary standards for other SCI-handling systems.

25X1

4. In June 1984, an interagency Computer Security Technology Panel was established to assess the application of computer security technologies against known operational deficiencies within Intelligence Community computer systems. The panel focused on what could be done, in the near term, with existing computer security technology and administrative/management actions to provide security upgrades for our "critical" systems. Specific emphasis was given to three areas of computer security vulnerability: authentication of

WARNING NOTICE
INTELLIGENCE SOURCES
OR METHODS INVOLVED

CL BY SIGNER
DECL OADR

25X1 [redacted]

SUBJECT: Reports on Computer Security for SCI-Handling Systems

users; accountability of operating actions; and labeling of SCI information. The findings and recommendations of the Technology Panel are provided to you for your use and comment (See Attachment 3). When these "action-oriented" recommendations are arrayed against the identified vulnerabilities of the "critical" systems and the threat against them, it will lead to a plan for significant improvement in Community COMPUSEC. I intend to pursue these recommendations, in coordination with other computer security initiatives, to
25X1 strengthen the protection of SCI material in computer-based systems. [redacted]

5. These documents are also being provided to the appropriate officials
25X1 with responsibilities assigned by NSDD/145. [redacted]

William J. Casey

Attachments:
25X1 1) [redacted]
2) Computer Security Technology Assessment Report
3) Uniform SAFEGUARDS for Protection of "Critical Systems" Processing Intelligence Information

25X1 [redacted]

SUBJECT: Reports on Computer Security for SCI-Handling Systems

Distribution:
Copy 1 - DCI (William J. Casey)
2 - SecDef (Caspar W. Weinberger)
3 - DDCI (John N. McMahon)
4 - EXDIR/CIA (Jim Taylor)
5 - ASD(C^{3}I) [redacted] 25X1
6 - D/INR (Hugh Montgomery)
7 - D/DIA (LtGen James A. Williams, USA)
8 - D/NSA (LtGen Lincoln D. Faurer, USAF)
9 - D/DNI (Rear Admiral John Butts, USN)
10 - Assistant Director, Intel. Div., FBI (Edward J. O'Malley)
11 - DOE/DAS, Intelligence (Charles Boykin)
12 - Treasury (Douglas Mulholland)
13 - Air Force, Under Secretary (Edward C. Aldridge, Jr.)
14 - Army/ACSI (LtGen William E. Odom, USA)
15 - Air Force/ACSI (MajGen James C. Pfautz, USAF)
16 - USMC/DI (BG Lloyd W. Smith, USMC)
17 - NSC (Ken deGraffenreid)
18 - National Security Advisor (Robert McFarlane)
19 - DUSD/P (Gen. Richard G. Stilwell, USA Ret.)
20 - Justice Dept (Mary C. Lawton)
21 - DOC (Irving P. Margulies)
22 - Chm/IPC/CIA (Richard Kerr)

25X1 1 - OS/C/ISSG [redacted] (w/att 2 only--3 copies)
25X1 1 - DIA/RSE [redacted] (w/att 2 only--15 copies)
1 - State (Lynn McNulty) w/att 2 only--2 copies)
1 - OSD (Gene Epperly) (w/att 2 only--3 copies)
25X1 1 - SECOM [redacted] (w/att 2 only--5 copies)
25X1 1 - [redacted] (w/att 2 only--5 copies)